

UNITED STATES DISTRICT COURT

for the
Eastern District of Tennessee

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

Electronic Devices recovered from the residence of Brent
DeSalvo and currently located at Container "EV", OSI
Detachment 106, Evidence Locker, Arnold Air Force Base,
Tullahoma, Tennessee 37389

Case No. ~~4:23-MJ-~~

1:23-mj-191-SKL

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search
of the following person or property located in the Eastern District of Tennessee

(identify the person or describe the property to be searched and give its location):

As set forth in the attached Affidavit, Electronic Devices recovered from the residence of Brent DeSalvo and currently
located at Container "EV", OSI Detachment 106, Evidence Locker, Arnold Air Force Base, Tullahoma, Tennessee 37389, as
set out in Attachment A, attached and incorporated herein.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property
described above, and that such search will reveal (identify the person or describe the property to be seized):

See Attachment B, attached and incorporated herein.

YOU ARE COMMANDED to execute this warrant on or before July 13, 2023 (not to exceed 14 days)

☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the
person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the
property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory
as required by law and promptly return this warrant and inventory to Hon. Susan K. Lee, U.S. Magistrate Judge
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C.
§ 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose
property, will be searched or seized (check the appropriate box)

☐ for days (not to exceed 30) ☐ until, the facts justifying, the later specific date of

Date and time issued:

June 29, 2023
6:20 p.m.

City and state:

Chattanooga, Tennessee

[Signature]
Judge's signature

Hon. Susan K. Lee, U.S. Magistrate Judge

Printed name and title

Return

Case No.:

4:23-MJ-

191

Date and time warrant executed:

30 Jan - 12 Jul 23

Copy of warrant and inventory left with:

OSI Det 106

Inventory made in the presence of:

OSI Det 106 Evidence Custodian - Kelsey Logan

Inventory of the property taken and name of any person(s) seized:

TSP

SEE ATTACHED

/TSP

TSP

/TSP

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date:

13 Jul 23



Executing officer's signature

Special Agent Trevor Osborn

Printed name and title

ATTACHMENT A

1. The property to be searched is a Toshiba Hard Drive, serial number: 95513250P; Toshiba Hard Drive, serial number: 96C34369A-1; Hitachi Hard Drive, serial number: DLH7SJNB-1; Seagate Hard Drive, serial number: 5RE26LL0-2; Maxtor Hard Drive, serial number: R20JVAYE; Maxtor Hard Drive, serial number: F12LJHHE-3; Western Digital Hard Drive, serial number: WMA2F; Western Digital Hard Drive, serial number: WCAATC010464; Western Digital Hard Drive, serial number: WMA6Y1263379-1; Unmarked Hard Drive, serial number: 6EG1EVP6; a Seagate External Hard Drive, serial number: NAOM2FQZ; a Seagate Hard Drive, serial number: 6RX6B5YB; a HP Hard Drive, serial number: B365P6A079T5; One cardboard box containing several hard drives; a Seagate Hard Drive, serial number: NAATPFX2; a Seagate Hard Drive, serial number: WXN1AB85Z9RY; a MyPassport External Hard Drive, serial number: NAA863E0; a ONN Hard Drive, serial number: 100003560; a Maxpro writing pen with attached flash drive; One box of multiple electronic memory storage chips derived from computer towers; a Samsung Galaxy S8 Cell Phone, FCOID: A3LSMG950U; a Samsung Cell Phone, model number unknown, IMEI: 357452522814468; Several Compact Discs, a Dell Laptop Computer, serial number: 221TWZ1; a Dell Inspiron Laptop, serial number: 00043726386389; 14 Thumb Drives collected in a black case; a HP Envy computer tower, serial number: 2MD61302TZ; a HP Laptop Computer, serial number: CND1Q3472L; a HP Laptop Computer, serial number: CND10348BR; a HP ProLiant Computer Tower, serial number: MX244500MX; a HP Pavilion Computer Tower, serial number: CNV6440K5L; a HP Z420 Computer Tower, serial number: 2UA4431ND9; a HP Z440 Computer Tower, serial number: 2UA5251RWR; a KVL-4000, serial number: 201CQH3355; Three SD Memory Cards, SanDisk, Wintec and Mad Catz; a Seagate NAS 4-bay hard drive reader serial number: NA6A50ZJ with three hard drives inside serial number's

W1H4597X, W1H45A85, W1H45A01; a Seagate NAS 4-bay hard drive reader serial number: NA6A50ZC with four hard drives inside, serial numbers: W1H45AWM, W1H45AZY, W1H4590M, W1H45AY5; a Motorola XTS5000 Portable Radio, serial number removed from device; a Windows 2012 R2 Thumb Drive; an unmarked Thumb Drive, silver and black in color; Five Thumb Drives identified as programming software for AAFB LMR communications systems and Tennessee Advanced Communications Network (TACN) communications systems; hereinafter the "Devices." The Devices are currently located at the OSI Det 106 Evidence Locker at 100 Kindel Drive, Ste. C305, AAFB, TN.

2. Items were seized based on the documentation included with this attachment.
3. This warrant authorizes the forensic examination of the Devices for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Devices described in Attachment A that relate to violations of Title 18 U.S.C. § 641, and involve DESALVO since his employment at AAFB, including:

- a. Computers or storage media used or able to be used as a means to commit the violations described above.
- b. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which are stored records or information that is otherwise called for by this warrant;
- c. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
- d. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- e. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crime(s) under investigation and to the computer user;
- f. evidence indicating the computer user's knowledge and/or intent as it relates to the crime(s) under investigation;
- g. evidence of the attachment to the Devices of other storage devices or similar containers for electronic evidence;
- h. evidence of the use of cloud storage, including Apple iCloud;
- i. evidence of programs (and associated data) that are designed to eliminate data from the Devices;
- j. evidence of the times the Devices were used;
- k. passwords, encryption keys, and other access devices that may be necessary to access the Devices;

- l. documentation and manuals that may be necessary to access the Devices or to conduct a forensic examination of the Devices or that show the operation of AAFB and other government communications systems;
- m. records of or information about Internet Protocol addresses used by the Devices;
- n. records of or information about the Devices' Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- o. contextual information necessary to understand the evidence described in this attachment;
- p. Routers, modems, and network equipment used to connect computers to the Internet.
- q. Records, information, and items relating to the ownership or use of the Devices and equipment, including sales receipts, bills for Internet access, and handwritten notes;
- r. Radio programming software and related identifying information pertaining to LMR communications systems;
- s. types, amounts, and prices of any sold radio equipment as well as dates, places, and amounts of specific transactions;
- t. any information related to the storage of electronic data belonging to AAFB;
- u. Records and information relating to the identity or location of the persons suspected of violating the statutes described above;
- v. all bank records, checks, credit card bills, account information, and other financial records associated to the sale of radio equipment.

2. Evidence of user attribution showing who used or owned the Devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

- a. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

The term “storage medium” includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.

3. During the execution of the search, law enforcement personnel are also specifically authorized to compel BRENT DESALVO, date of birth 20 Dec 74, to provide biometric features, including pressing his fingers (including thumbs) against and/or putting his face before the sensor, or any other security feature requiring biometric recognition, of any of the Devices found at the PREMISES which are capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities of the offense(s) as described in the search warrant affidavit and warrant attachments, for the purpose of attempting to unlock the Devices’ security features in order to search the contents as authorized by this warrant.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, OSI may deliver a complete copy of the seized or copied

electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

Search Warrant Return

Date: 13 Jul 23

Date Range: 30 Jun 2023 – 12 Jul 2023

Search Conducted By: Special Agent (SA) Trevor Osborn and Evidence Custodian (EC) Kelsey Logan, OSI Det 106, Arnold AFB (AAFB), TN

30 Jun 2023

Item # 4TFHD: Attempted extraction. The attempt was unsuccessful. Item is being sent to DC3 (forensic lab) for analysis.

Item # XCWQ8: Contained two pictures of two unidentified children sitting on Santa Claus' lap. Not relevant to the investigation. Item will be released.

Item # 57FWJ: Evidence item contained 14 USB drives.

1. Red Avaya USB: Contained electronic system keys, SUBJECT's former supervisors resume that included his home address, router folders, and AAFB LMR Trunk System files, AAFB network switch and router configurations and AAFB information comingled with nude photographs of an unidentified female. Upon reviewing some of the Motorola radio programming files a warning banner was identified for "U.S. Government Systems".
2. Gray Motorola USB: Contained boot folders, radio programming files, APX portable and mobile radio CPS files for Motorola (Astro 25 system) (CPS application allows the viewing and use of radio code plugs), AETC eLMR administrative passwords, and electronic system keys. All items were extracted and placed in electronic storage as a working copy.

6 Jul 2023

Item # 57FWJ: This item was reopened to examine the remaining USB drives. The Red Avaya USB that was previously opened on 30 Jun 2023, was reopened for extraction via Falcon.

At 1431, after consulting with DC3, SA OSBORN and EC LOGAN, tested the extraction software to verify write block was enabled to begin previewing evidence for relevance to the case, rather than extracting due to the amount of digital evidence, time constraints, and the amount of electronic storage needed to conduct extractions. SA OSBORN confirmed write block was enabled, and evidence was able to be previewed on an OSI Det 106 standalone laptop.

3. Purple USB drive marked "Desalvo": Contained AAFB radio programming software/files, Windows key finder software, and AAFB building specific configurations and schematics.

4. Orange USB drive marked "Desalvo": Contained boot and driver files, along with various computer configuration settings.
5. Pink USB drive marked "Desalvo": Contained AAFB network switch sheets, the 2020 AETC eLMR password sheets, 2021 AAFB fleet map, electronic system keys, Motorola Astro 25 radio programming software and radio programming information, licensing information, IP address sheet. Additionally, the drive contained an AETC eLMR talk group file that contained talk groups for the 17 DoD installations under the AETC eLMR system.
6. Black USB drive marked "Desalvo": Blank. Not relevant to the investigation.
7. White USB drive marked "Desalvo": Contained Motorola Astro 25 radio programming software and information.
8. Yellow USB drive marked "Desalvo": Contained computer programming information.
9. Blue USB drive marked "Desalvo": Contained computer programming information.
10. Green drive USB marked "Desalvo": Contained Motorola Astro 25 mobile/portable radio depo and radio code plugs, Astro 25 computer programming, system keys, file folder labeled "Arnold AFB software", AAFB Giant Voice programming, and unrelated .vip song tracks and personal audio recordings.
11. Pink USB drive marked "Desalvo": Contained KVL encryption keys, and Bit Locker drive encryption recovery keys.
12. Green USB drive marked "Desalvo": Contained a warranty picture. Not relevant to the investigation.
13. Burnt red USB drive marked "Desalvo": This USB was unreadable and will be sent to DC3 (forensic lab) for full extraction.
14. Red USB drive marked "Deslavo": Contained KVL files, Motorola Astro 25 programming software, AAFB ethernet connectivity site map, radio programming software, and electronic system keys.

Item # 89XQ3: Contained Motorola Astro 25 computer programming, RMF sites, LMR sites, Motorola APX radio depo, AAFB IP plan, Arnold AFB fleet map session, unrelated personal music files, OBX-tech information (Prior contract for LMR on AAFB), Motorola passwords for AAFB, 2021 AETC eLMR Lackland password sheet, Motorola software.

Item # 3HEBG: Contained 2022 AAFB code plugs, system keys, APX radio software, AAFB software, Motorola Astro 25 mobile/portable radio systems, Tennessee TACN radio programming files, unrelated personal audio files, AAFB advanced system keys, Tennessee radio programming, AETC eLMR Lackland password sheet, 2021 and 2022 AAFB fleet map, local law enforcement radio programming files, Windows key recovery software.

Item # XCWQ8: This item was unsealed for a 2nd time however it was already extracted on 30 Jun 23 and showed no relevance to the case.

Item # F1E7Q: This item is a plastic container that contained several USB drives, SD memory cards, and other computer/data sticks.

1. Black USB drive with 1 GB China sticker: It was unable to be viewed as it states it needs to be formatted. This USB will be sent to DC3 (forensic lab) for a full extraction.
2. Blue and silver "InfoTrust" USB drive: Item was unable to be viewed. This drive will be sent to DC3 (forensic lab) for a full extraction.
3. "Gillette" advertisement thumb drive: Item was unable to be viewed. This drive will be sent to DC3 (forensic lab) for a full extraction.
4. Blue DT101 G2 USB drive: Contained CNC Sand and Stone Radio Inventory, Dicks Sporting Goods Repeater map, and Lockheed Martin frequency map with schematics.
5. "Wal-Mart" USB drive: This drive was unable to be read and will be sent to DC3 (forensic lab) for a full extraction.
6. "American Airlines" USB drive: This drive was unable to be read and will be forwarded to DC3 (forensic lab) for a full extraction.
7. Black and red Sandisk USB drive: Contained Motorola programming software, site surveys, other radio software.
8. Black HP USB drive with clear face: This drive was unable to be read and will be forwarded to DC3 (forensic lab) for a full extraction.
9. Tennessee 811 USB drive: Contained radio programming and "CTB" files.
10. Blue "Staples" flash drive: Contained concert photos and videos for a band called "Demon Kat". Not relevant to the investigation.
11. PNY Technologies Attache USB drive: Contained one folder titled "11" which contained no files. Not relevant to the investigation.

7 Jul 2023

Item # 49RMG: This item was an external hard drive named "Honeys Passport" located inside a black case labeled "USA Microtech Arnold AFB ELMR GTR." It contained Honey Desalvo's personal folders and files, a folder titled "DesktopInstaller_4000" that contained Motorola Installation packages, KVL and Installer files that upon opening read "CONFIDENTIAL RESTRICTED" in the banner, SUBJECT and Honey Desalvo's PII, a file folder dedicated to "KVL" and subfolder titled "Keyfiles" with KVL software and installation packages and within was Motorol_Astro.KeyManagement.d11.

Item # 3WECR: This item consisted of 3 external hard drives.

1. Black external drive with "WD" on front. This drive was unable to be opened due to bitlocker and password protection. It will be forwarded to DC3 (forensic lab) for a full extraction.
2. Black external drive with "717" in white and labeled "Property of Brent Desalvo". This drive could not be opened due to bitlocker and will be forwarded to DC3 (forensic lab) for a full extraction.
3. Black external drive with white 20 (unreadable) HS and labeled "Property of Brent Desalvo." This drive contained a file folder titled "Arnold AFB completed." There were file folders for specific buildings on AAFB including testing facilities - Fire, Security, Command, APTU, PWT, VKF, ASTF, AAFB ELMR GTR Astro 7.17, Motorola programming and software guides, KVL software patches, AAFB radio programming information, electronic system key files, Backup and restore packages, code plugs for the "pipe shop", and Windows key finder software.

Item # 19EK3: This item consisted of 32 discs.

1. Silver CD-RW labeled Dell Utilities: Contained data files. Not relevant to the investigation.
2. Memorex labeled Windows XP in red: Contained Windows files. Not relevant to the investigation.
3. Silver Memorex CD-R: Contained Alfresco Community Installer. Not relevant to the investigation.
4. Gold Memorex CD-R: Contained Motorola Installation guides.
5. Silver Imation disc labeled Win7SP1 in black: Contained Windows Installation software. Not relevant to the investigation.
6. Silver Verbatim CD-R labeled Lookout v6.02 M62X86762: Contained Lookout software.
7. Silver Verbatim CD-R labeled Zetron Model 1730.1732 Configuration Utility v2.0: Contained Zetron software for radio programming.

8. Silver Memorex DCD+R labeled Red Hat 5.8 in red: Contained Red Hat 5.8 software for radio programming.
9. Gold Sony CD-R labeled Tullahoma 22 & 23 Aug 08 Gentry Site: Contained photos of AAFB Gentry site-communications tower.
10. Orange and silver disc labeled Office 2003 in red: Contained Office 2003 software. Not relevant to the investigation.
11. Silver Sony CD-R labeled Digi 115B: Contained Digi software.
12. Silver Verbatim disc labeled "Brent" in red: Contained nude photographs of unidentified females. Not relevant to the investigation.
13. Silver Verbatim disc labeled "Boodie Bungalow" in black: Contained nude photographs of unidentified females. Not relevant to the investigation.
14. Silver Imation disc labeled G97FV-GVB6M-QBRXH-9B4JD-Y2G9F Windows 7 64 bit: Contained Windows software. Not relevant to the investigation.
15. Orange and silver disc labeled 70_1088: Contained XTRHH software. Not relevant to the investigation.
16. White Verbatim disc labeled EF Johnson: Contained EF Johnson Portable Radio Programming software.
17. Gold Memorex CD-R: Contained no files. Not relevant to the investigation.
18. Gold Memorex Music CD-R: Contained no files. Not relevant to the investigation.
19. Silver Verbatim CD-R labeled "Mail Backup": Contained Arnold SOW, AAFB map, 2006 excessed equipment list, local frequency list, "old" AAFB LMR information.
20. Silver CD with no markings: Contained 2017 Motorola software A7.17.2
21. Silver Verbatim labeled MCD 5000 Red Hat Linux 5.8 kickstart: Contained Motorola Linux software.
22. Gold Memorex Music CD-R with no label: Contained Windows based Ubuntu installer software.
23. Gold Memorex CD-R labeled XP Office Plus CD key: Contained XP Office software. Not relevant to the investigation.
24. Silver Verbatim CD-R labeled Zetron RTU Test: Contained Zetron software.

25. Silver Verbatim CD-R labeled Ritron DTX plus series v2.58: Contained Ritron radio software.
26. Silver Magnavox disc labeled For Whelen 2900's: Contained SDPTS file folder.
27. Gold Memorex Music CD-R labeled DSET-Win: Contained Dell DSET software. Not relevant to the investigation.
28. Gold Memorex CD-R labeled Travel Plus 4 Repeater2005-2206: Contained Travel Plus 4 Repeater software for radio programming.
29. Orange and silver Maxwell disc labeled Office 2003: Contained office software. Not relevant to the investigation.
30. Silver Memorex CD-R labeled SharePoint 2010 64 bit: Contained SharePoint software. Not relevant to the investigation.
31. Gold and white Prime Peripherals CD-R labeled 1/02/01 Windows 2000 RVJPW-VTBY3-9MXGM-XKQBM-2W3PD: Contained windows software. Not relevant to the investigation.
32. Orange and silver Maxwell CD-R labeled XP Office w/ Front Page & key: Contained XP office software. Not relevant to the investigation.

Item # 2NG7P: Silver Verbatim CD-R labeled code plugs CPS SYS Keys: Contained electronic system keys.

Item # B7RUG: This item consisted of 18 discs in plastic or paper cases.

1. Blue case labeled Magix Files: Contained music player/manager. Not relevant to the investigation.
2. Black and clear Maxwell CD-R case labeled Cakewalk GTPro v.3: Contained music software. Not relevant to the investigation.
3. Black and clear case labeled Cubase LE4 Tutorial: Contained Cubase LE4 Tutorial. Not relevant to the investigation.
4. Pink and clear case labeled Adam Sandler: Contained personal audio files. Not relevant to the investigation.
5. Black and clear case labeled Wanda Jackson: Contained audio files, unable to play. Not relevant to the investigation.
6. Pink and clear case labeled Greatest Hist 1-19-12: Disc was unable to be read. Deemed not relevant to the investigation.

7. White paper case with no label: Contained audio files. Not relevant to the investigation.
8. White and blue Memorex paper case labeled Samplitude: Contained audio software. Not relevant to the investigation.
9. Black and clear case with no label: Contained audio files. Not relevant to the investigation.
10. Blue and clear case labeled Davis Alan Coe Stuff: Contained audio files. Not relevant to the investigation.
11. Black and clear case labeled Cubase LE BBD0X-AAMZT-FS1QD-Q1FLA-AWBHA: Contained Cubase software. Not relevant to the investigation.
12. Blue and clear case labeled David Alan Coe Stuff: Contained audio files. Not relevant to the investigation.
13. Black and clear case labeled John Michael Montgomery: Contained audio files. Not relevant to the investigation.
14. Black and clear Imation case labeled Corona Mix 7: Contained audio files. Not relevant to the investigation.
15. White and clear case labeled Dace to the Music: Contained audio files. Not relevant to the investigation.
16. Black and clear case labeled Steve Miller Joe Cocker: Contained audio files. Not relevant to the investigation.
17. Pink and clear case labeled Greatest Hits 1-19-2012: Contained audio files. Not relevant to the investigation.
18. Orange and clear case labeled Elvis: Contained audio files. Not relevant to the investigation.

Item # EDJX0: This item contained 29 discs.

1. Green Motorola disc labeled Arnold AFB: Contained license key.
2. White and clear case with white disc: Disc unreadable. This item will be forwarded to DC3 (forensic lab) for a full extraction.
3. White and clear case with disc labeled Inside Out Chic Corea: Contained audio files. Not relevant to the investigation.

4. White Microsoft Windows Server 2012 R2 Essentials Disc with CCSDSVR1 label. Not relevant to the investigation.
5. Green Motorola Site Rptr Base Radio Software Disc.
6. Blue Motorola Astro 25 Integrated Voice and Data System Disc.
7. Red Motorola McAfee Standalone Local Media Disc.
8. Blue Motorola McAfee Standalone Local Media Disc.
9. Blue Motorola GMC/GWS GUI and SDM3000 Config S/W and Doc Disc.
10. Blue Motorola All SDM3000 RTU, SNT, MCC7500 Aux 10 FW Disc.
11. Blue Motorola Configuration Service Software (CSS) Disc.
12. Blue Motorola KVL 4000 Key Variable Loader Disc.
13. Green Motorola VPM Software Disc.
14. Case containing 2 Green Motorola VPM Software discs.
15. Clear case containing 1 blue Motorola All SDM3000 RTU, SNT, MCC7500 Aux 10 FW Disc.
16. Blue Motorola Configuration Service Software (CSS) Disc.
17. Red Motorola Windows Common OS Box Profile Disc.
18. Case contained 2 discs. A blue Motorola Microsoft Windows Server, unable to be read and a disc labeled Motorola Solutions CSO, CCSI Staging Documentation "USA Arnold AFB".
19. Case containing 2 green Motorola MCC 7500 Software discs.
20. Clear case labeled "B Desalvo" with disc labeled Motorola CPS and Tuner Disc.
21. White CD labeled Radio Soft ComStudy 2.2
22. Red Motorola windows Common OS Box Profile Disc.
23. Red Motorola Windows Supplemental Full Config Disc.
24. Red Motorola Windows 10 v 1607 OS Image Disc.
25. Clear case containing a red Motorola Windows Common OS Box Profile Disc

26. Clear case containing red Motorola Windows Common OS Box Profile Disc.

10 July 2023

Item #LF97K: This item of evidence contained 5 USB drives.

1. Three blue USB drives with two white labels, one on each side, and a Coffee County Sheriff's Office Evidence Tag attached. The first blue drive contained a label on one side titled "Master System Key – USAF Land Mobil Radio Shop." The second blue USB contained a label on one side titled "TACN" which is short for the Tennessee Advanced Communications Network. The third blue drive was not specifically labeled. These drives at the time of collection and preview by Coffee County Sheriff's Office were identified as radio trunk systems. These drives were unable to be viewed by OSI Det 106 due to needing specific radio programming software to view contents. After coordination with AAFB LMR representatives, the drives can be read on their software systems. The drives titles "USAF Land Mobile Radio Shop" and "TACN" are deemed to be State and Federal Government property.
2. The other two drives were black in color and labeled "Windows 2012" and "Windows 2019". The windows 2012 drive contained radio programming software and information and open-source applications relevant to the investigation. The windows 2019 drive contained computer programming files possibly associated to Windows 2019 computer software and configurations.

Item # 1KM70 – Item could not be viewed due to PIN code authorization. This item will be sent to DC3 (forensic lab) for analysis.

Item # A0LWM - Item could not be viewed due to PIN code authorization. This item will be sent to DC3 (forensic lab) for analysis.

12 Jul 2023

Item # P113Y – Item to be sent to DC3 (forensic lab) for extraction.

Item # 58XDN – Item to be sent to DC3 (forensic lab) for extraction.

Item # 2LWEK – Item to be sent to DC3 (forensic lab) for extraction.

Item # MY5NA – Item to be sent to DC3 (forensic lab) for extraction.

Item # 1RWDQ – Item to be sent to DC3 (forensic lab) for extraction.

Item # RF5RA – Item to be sent to DC3 (forensic lab) for extraction.

Item # CWL3Y – Item to be sent to DC3 (forensic lab) for extraction.

Item # 8CNJ2 – Item to be sent to DC3 (forensic lab) for extraction.

Item # 8WXF2 – Item to be sent to DC3 (forensic lab) for extraction.

Item # RMKW2 – Item to be sent to DC3 (forensic lab) for extraction.

Item # M7YYE – Item to be sent to DC3 (forensic lab) for extraction.

Item # TJQR7 – Item to be sent to DC3 (forensic lab) for extraction.

Item # 5NY50 – Item to be sent to DC3 (forensic lab) for extraction.

Item # MP5TJ – Item to be sent to DC3 (forensic lab) for extraction.

Item # JKDP1 – Item to be sent to DC3 (forensic lab) for extraction.

Item # TH533 – Item to be sent to DC3 (forensic lab) for extraction.

Item # BEY77 – Item to be sent to DC3 (forensic lab) for extraction.

Item # A0LWM – As previously stated, item to be sent to DC3 (forensic lab) for extraction.

Item # 1KM70 – As previously stated, item to be sent to DC3 (forensic lab) for extraction.

Item # 9EXLT – Item to be sent to DC3 (forensic lab) for extraction.

Item # 4TFHD – As previously stated, item to be sent to DC3 (forensic lab) for extraction.

Item # JNBT5 – Item was unable to be viewed. Item will be sent to DC3 (forensic lab) for extraction.

Item # 3WECR – On 7 Jul 23 this item was unsealed and two on the external drives were unable to be read. An attempt was going to be made based off recovered Bitlocker recovery keys, however, after speaking with SA ANDREW WATSON, Digital Forensic Consultant, OSI 2 FIS, JB Andrews, MD, he recommended sending the drives to DC3 (forensic lab) for extraction.

Item # UMRR7 – This item contained 3 SD memory cards. The SD memory cards were viewed using the same forensic extraction/preview software with write block protection.


1. SanDisk 256 MB: Contained different applications and files that could not be viewed without specific software. This item will be sent to DC3 (forensic lab) for extraction.
2. WINTEC filemate SDHC Flash Card 8 GB: Contained audio files. Not relevant to the investigation.
3. MEMORY CUBE: Used for GAMECUBE video gaming console as a memory card. Not relevant to the investigation.

Item # F1E7Q – On 6 Jul 23, this item was previously opened to view the drives that were located in the container. On 12 Jul 23, it was reopened to view the (12) SD memory cards, (1) Memory Stick, and (6) SIM Cards.

1. PNY CompactFlash 256MB: Contained different web applications and configuration settings. Item to be sent to DC3 (forensic lab) for extraction.

2. Cisco Systems with label 17-6715-01 barcode 32MB: Blank. Not relevant to the investigation.
3. Micro SD 1GB Delkin Devices: Personal photographs. Not relevant to the investigation.
4. Micro SD 1GB with small white label partially torn: AAFB Giant Voice (Emergency Warning System) Audio Files.
5. Micro SD HC 8 GB with pink dot: Personal voicemails, including one from Anthony "Delmarini" about a job application for Motorola Federal Service Team (FST) in 2017, in addition to personal photos and documents. The voicemail may be of interest to pursue leads, the rest of the files were not relevant to the investigation.
6. SanDisk Ultra Plus 32 GB: Blank. Not relevant to the investigation.
7. PNY SD Lock 256MB: Item stated, "Disc has to be formatted before use, the volume does not contain a recognized file driver" and that the volume might be corrupted. Item will be sent to DC3 (forensic lab) for extraction.
8. SONY Memory Stick Pro Duo 1GB: Contained decoding and Motorola programming software.
9. Samsung Micro SD 8GB: Item stated, "Please plug into USB." Unable to be viewed. Item will be sent to DC3 (forensic lab) for extraction.
10. Transcend Micro SD 2GB: Unable to be viewed. Item will be sent to DC3 (forensic lab) for extraction.
11. Micro SD Ultimate 3.0 8GB: Unable to be viewed. Item will be sent to DC3 (forensic lab) for extraction.
12. SanDisk Micro SD 1GB: Unable to be viewed. Item will be sent to DC3 (forensic lab) for extraction.
13. Black Memory Stick: Unable to be viewed. Item will be sent to DC3 (forensic lab) for extraction.
14. The remaining (6) SIM cards were unable to be viewed. Items will be sent to DC3 (forensic lab) for extraction.

DATE: 13 Jul 23



Special Agent, Trevor Osborn